証跡管理基盤におけるサービス事実証明のための要件に関する一検討

橋本 正一　　坂本 昌史　　中原 慎一　　平田 真一

NTT 情報流通プラットフォーム研究所
180-8585 東京都武蔵野市緑町 3-9-11
{hashimoto.shoichi, sakamoto.masanobu, nakahara.shinichi, hirata.shinichi}@lab.ntt.co.jp

あらまし　安心安全なネットワークサービスの実現には，認証等のサービス提供時のセキュリティと共に，その事実を必要に応じて証明するサービス提供後のセキュリティも重要となる．近年，内部統制等の要求からログ管理の重要性が高まっているが，既存のログ管理は組織内の不正検出や監査報告等が目的とされ，サービス事実を当事者に対して証明することは想定されていない．筆者らは，ネットワーク上で複数主体により提供されるサービス事実を証明するための証跡管理基盤について検討しており，本稿では，サービス事実証明に特有な証跡情報への要件となる(1)複数証跡情報によるサービス事実の証明，および(2)証跡情報に対する客観性の向上について述べた後，その実現のための技術要件について述べる．

A Study on Requirements for Proof of the Service Fact on the Digital Evidence Management Base

Shoichi Hashimoto　　Masanobu Sakamoto　　Shinichi Nakahara　　Shinichi Hirata

NTT Information Sharing Platform Laboratories
3-9-11 Midori-cho Musashino-Shi Tokyo, 180-8585 Japan
{hashimoto.shoichi, sakamoto.masanobu, nakahara.shinichi, hirata.shinichi}@lab.ntt.co.jp

Abstract In late years the importance of the log management is spreading by necessity of the internal control. The purposes of most of the existing log management products are to detect injustice in the organization and to generate the audit report, and it is not assumed that they prove the fact of the service that happened. So we have discussed the technical requirements of the digital evidence management base to prove the fact of the service offered by service providers on network. In this paper, we propose requirements in particular for the evidence information to prove the fact of the service, furthermore, we describe the technical elements to realize that requirements.

1　はじめに

ブロードバンド環境の普及や，ユビキタス環境の進展に加え，SaaS やクラウド等の新たなサービス提供基盤の技術開発や整備が進められる中，ネットワークを介した多様な情報流通やサービス提供が広く行われるようになっている．このようなネットワーク上で展開されるサービスを

安心安全なサービスとして実現するためには，サービス提供時における認証や暗号化等によるセキュリティの担保に加えて，サービス提供の事後においても，サービス提供が行われたことの事実や，適切にシステム運用が行われたことの事実を，必要に応じていつでもサービスの利用者や提供者が確認あるいは証明できることの担保も重要な要素となる．

事後における証明や監査への対応を実現するための技術の1つとして，証跡管理技術が挙げられる．証跡管理技術は，近年，特に企業におけるJSOX法やISMS対応に関連する監査対応やデジタルフォレンジック対策等の内部統制への要求に絡んで，その必要性，重要性の認識が高まっており，これらに関連する研究[1][2]や製品開発が活発化している．

しかしながら，現状の証跡管理製品の多くは，主に内部統制を目的として，組織内の各システムを対象にあらゆるログを収集，分析することによって，不正検出や内部監査用のレポート作成等を行うなどといった，組織内に閉じた範囲で利用されることを想定したものとなっている．

そこで筆者らは，ネットワークを介したサービスにかかる利用者とサービス提供者間の紛争の解決や防止等を目的として，サービスが行われたことの事実（サービス事実）を証明するための証跡情報を収集管理し，これを長期にわたり，いつでも確認，提示可能となる証跡管理基盤について検討を進めている．本証跡管理基盤は，同一組織内に閉じない，利用者と複数の異なるサービス提供者を対象範囲とし，サービスにおける各プロセスの動作の説明に適した証跡情報を，選択的に収集，管理しようとする点で，既存の証跡管理とは異なる特徴を有するものである．

本稿では，ネットワークを介したサービス事実を証明可能な証跡管理基盤の実現に向けて，サービス事実の証明に求められる証跡情報に対する特有な要件として，(1)複数証跡情報によるサービス事実の証明，および(2) 証跡情報に対する客観性の向上 について述べた後，これらの要件を満たした証跡情報を収集管理するために求められる技術要件について述べる．

2 サービス事実証明のための証跡管理基盤とは

本章では，本稿の検討対象であるサービス事実を証明するための証跡管理基盤の構成イメージ，基本機能等の全体像を説明する．

サービス事実を証明するための証跡管理基盤とは，図 1 に示すように，サービス利用者とサービス提供者との間でネットワークを介したサービス提供が行われる環境において，サービス事実が発生した延長上でその証跡を収集，蓄積し，後日，サービスの当事者（利用者，サービス提供者等)や監査人等からの要求に応じて，蓄積した証跡情報を提示可能とするための基盤サービスと考えている．

証跡管理基盤を構成する基本機能としては，証跡情報の収集，検証，保証化，蓄積管理の機能区分に分類され，それぞれ以下の役割を持った機能として構成される．

- 証跡収集
  証明したい事象の発生事実の説明に必要な証跡情報を収集するための機能
- 証跡検証
  取得した証跡情報の正当性を検証し，当座の事実を確認，確定するための機能
- 証跡保証化
  取得した証跡情報の正当性を維持し，長期にわたりその正当性を証明可能とするための機能
- 証跡蓄積管理
  取得した証跡情報を長期にわたり蓄積管理し，要求に応じて証跡情報の検索，閲覧，分析，証明，検証等を行うための機能

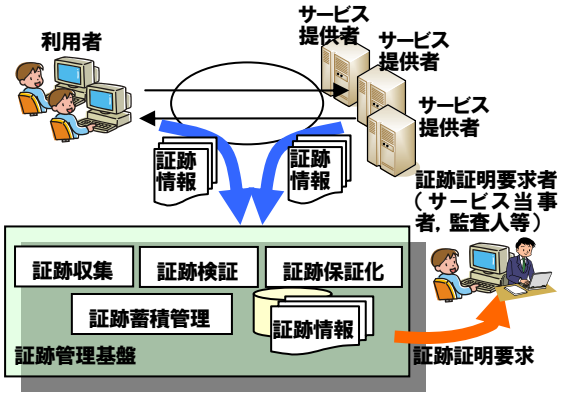

図 1 証跡管理基盤の概要イメージ

3 サービス事実証明のための証跡情報への要件

本稿では，サービス事実証明のための証跡管理基盤の実現に向けた検討の 1 つとして，収集管理すべき証跡情報に対する要件にフォーカスして検討を行った．

本章では，サービス事実の証明に有用な証跡情報を収集管理するために，通常のログ収集に比して，証跡情報に対してどのような要件が考慮されるべきかについて述べる．

3.1 複数証跡情報によるサービス事実の証明

利用者とサービス提供者との間でやり取りされるサービスの形態は様々に存在するが，一般にサービス事実の証明に対する要求として，利用者側においては，サービス提供者から受領したサービス結果を，サービス提供者が否認することがないよう，後日にわたって証明したいという要求が発生し，サービス提供者側においては，利用者がサービス事実を否認することがないよう，あるいは,サービス提供者自身の運用の正当性を外部に対して主張するために，利用者からの要求に基づき，適切にサービスを提供したことを後日にわたり証明したいという要求が発生するものと考えられる．

そこで本稿では，上記に示した利用者，サービス提供者の双方の要求を満たしたサービス事実の証明を実現するため，利用者によるサービス要求から，その要求に対するサービス結果が返されるまでに行われた一連のプロセスの発生事実をサービス事実とし，その事実を証明することをサービス事実の証明とすることとした．

サービス事実の証明を上記のように捉えた場合，その証明のために収集管理すべき証跡情報に対する要件としては，時刻や処理結果にかかる情報をテキストベースで収集する通常のログ収集ではカバーされていない，以下に示すサービス事実証明に特有の要件の考慮が求められる．

(1)サービスが複数プロセスにより構成されることの考慮

一般に利用者とサービス提供者との間で行われるサービスにおけるやり取りは，サービスサーバへのアクセス，認証，サービス要求，要求に対する処理，サービス結果の生成，提示などといった複数のプロセスで構成されている．サービス事実の証明においては，前述のように，サービスが適切なプロセスを経て完了したことの事実を証明できる必要があることから，サービス内で実行される各プロセスとの間で，各プロセスの動作が適切であることを説明可能な情報を証跡情報として収集するとともに，これらの証跡情報を証明対象のサービスにかかる一連の証跡情報として紐付けて残すことが求められる．

具体的には，利用者とサービス提供者との間でやり取りされる上記で挙げたような各プロセスにおいて，入出力情報やプロセス結果などといった，通常のテキストベースのログとは異なる，各プロセスの動作を表す情報を証跡情報として収集し，他のプロセスにおける証跡情報と紐付けて管理することが考えられる．

(2)異なるサービスが連携してサービス提供されることの考慮

(1)に関連して，利用者からのサービス要求に対して，複数の異なるサービスが連携してサー

ビスが提供されるようなケースでは，サービス提供者間でも利害関係が発生しうることから，各サービスの責任範囲において，各サービス提供者が適切にサービスを実行したことの事実を表す証跡情報が求められると考えられる．したがって，各証跡情報がどのサービス(サービス提供者)により生成されたのかといった各証跡情報の生成主体を確認するための情報や，どのサービスとの連携が行われたのかといったサービスの連携先に関する情報，さらには，各証跡情報がどの一連のサービスの中で発生したのかなどの情報を残すことが求められる．(図 2)

具体的には，例えば，官民連携における行政手続きのワンストップサービスなどのように，複数のサービスへのアクセス窓口となるポータルサービスのサービス提供者，認証サービスを提供するサービス提供者，実際の個別のサービスを提供するサービス提供者がそれぞれ異なるような場合に，ポータルを介したサービス要求から，認証を経てバックエンドの各サービスが適切に行われたことの事実を証明するための証跡情報を収集管理する場合などが相当し，各証跡情報に対して，生成元である各サービス提供者との紐付け情報や，サービス間の I/F における入出力情報や入出力先情報，各サービスのサービス結果情報，上記のポータルサービス，認証サービス，個別サービスの各サービスで生成された一連の証跡情報を紐付けるための情報などの収集が求められる．

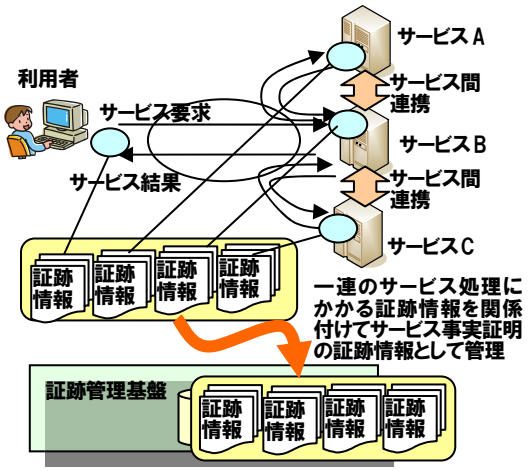

図 2 複数証跡情報によるサービス事実の証明

3.2 証跡情報に対する客観性の向上

内部監査や内部の不正検出を目的とした組織内に閉じた証跡管理と異なり，利用者とサービス提供者が互いに相手の否認防止を目的とした本稿で対象の証跡管理においては，証跡情報に対して，利害関係者(利用者，サービス提供者)が共に信頼できる,より高い証拠性が求められる．

こうした課題認識に対して，間形らは，証拠法や訴訟手続，仮想事例等をもとにした検討により，デジタル証拠の法的証明力を高めるための要件として，13の要件を提示している[3]．さらに，文献[3]では，これらの要件を満たす際には，信頼できる第三者による証明によって，デジタル証拠の証明力の安定性を補強する必要性があるとし，その証明方法として，デジタル証拠自体に第三者の証明が包含されていることが望ましいと言及している．

第三者の証明を含んだ情報としては，PKIにおけるデジタル署名やタイムスタンプが有効となりうる．デジタル署名は，署名対象情報に対する完全性と関与した当事者を，第三者である認証局(CA：Certification Authority)が発行する公開鍵証明書により証明されるものであることから，文献[3]における要件4(記録した主体が何かを証明できること)や，要件6(記録の完全性を証明できること)について，証拠情報の証明力を補強するものとなる．また，タイムスタンプは，タイムスタンプ対象情報に対する存在事実とその日時を第三者であるタイムスタンプ局(TSA：Time-Stamping Authority)が証明するものであることから，文献[3]における要件3(記録の実在を証明できること)や，要件5(記録した日時を証明できること)について，証拠情報の証明力を補強するものとなる．

そこで本節では，サービス事実証明のための証跡情報の収集において，証跡情報の証明力を補強するための情報として，デジタル署名やタイムスタンプを証跡情報に含めるための収集における要件について述べる．

サービス事実の証明においては，証跡情報を生成する主体として，サービスの当事者である利

用者やサービス提供者が存在し，一連のサービス処理において収集される証跡情報の中には，それぞれが相手の否認を防止する観点で，生成主体の証明(特定)が重要となる証跡情報が存在することが想定される．

したがって，このような証跡情報に対しては，証跡情報を生成あるいは収集するタイミングで，生成主体により証跡情報に対するデジタル署名を生成し，証跡情報とあわせてデジタル署名を収集できることが有効である．そしてさらに，収集したタイミングで，これらの情報に対するタイムスタンプをタイムスタンプ局から取得し，証跡情報に含めることにより，デジタル署名を含む証跡情報に対して，その存在日時の事実を第三者の証明により補強することが可能となる．

具体的に，生成主体の証明（特定）が求められる証跡情報としては，例えば，利用者が生成するサービス要求の内容を示す情報や，サービス提供者が生成するサービス結果の内容を示す情報が挙げられ，これらに対して，それぞれ情報の生成主体である利用者およびサービス提供者がデジタル署名を生成し，これを収集しておくことが考えられる．

4　証跡情報の収集管理にかかる技術要件

本章では，3 章で述べた要件を考慮した証跡情報を収集管理するために求められる技術について述べる．

4.1　複数証跡情報の連携

3.1 では，サービス事実を証明するための証跡情報に求める要件として，サービス要求からその要求に対するサービス結果が生成，提示されるまでの当該サービスにかかる一連のプロセスについて，各プロセスが確かに適切に動作したこと（プロセスの完全性）を表す情報を証跡情報として収集する必要があり，そのために通常のログ収集ではカバーされていないサービス事実証明特有の考慮すべき要件について述べた．

以下では，上記 3.1 で述べた要件を満たすために求められる技術について述べる．

(1)複数証跡情報を連携させるためのトランザクション管理

サービス要求からその要求に対するサービス結果の生成，提示に至るまでの各プロセスにかかる証跡情報を一連のサービス事実に紐付けて収集管理するためには，サービスの開始から終了までのサービス単位を事前に定義し，サービスの開始および終了の契機を管理しながら，収集した証跡情報を管理対象のサービスと紐付けるためのトランザクション管理が求められる．また，各プロセスが異なるサーバ上で実行される場合には，証跡情報の順序性保証のための各サーバ間の時刻同期の考慮も求められる．

(2)証跡情報の生成元の識別，認証

異なるサービスが連携してサービス提供される場合には，各サービスの責任範囲において，各サービス提供者が適切にサービスを実行したことの事実を表す証跡情報が求められ，証跡情報とサービス（サービス提供者）との紐付けが重要となる．したがって，上記(1)に加えて，証跡情報の収集過程において，証跡情報の生成元のサービス（サービス提供者）の識別，認証が求められる．具体的には，例えば，生成元であるサービス提供者と間の証跡情報の収集のためのコネクション形成時における認証の実施や，証跡情報に付与されたデジタル署名の検証による実現が考えられる．

(3)多様な証跡情報に対する統一的管理

プロセスの動作を表す情報を証跡情報として収集管理するためには，通常のテキストベースのログ情報だけでなく，やり取りされたデータや業務電文等のトランザクションデータを証跡情報として収集管理することが求められ，収集の I/F や証跡情報の蓄積，あるいは蓄積された証跡情報を証明する際の出力 I/F において，

多様なデータ形式を統一的に扱うためのメタ情報を含むデータ構造化技術が求められる.

4.2 証跡情報へのデジタル署名・タイムスタンプの適用

3.2 では証跡情報に対する客観性を向上させるため，証跡情報に対してデジタル署名を生成して証跡情報に含めることについて述べた.

以下では，証跡情報に対してデジタル署名やタイムスタンプを付与する際に求められる技術について述べる.

(1)証跡情報の収集処理やサービスへの影響を抑えた署名生成／検証処理

証跡情報に対する当事者(利用者やサービス提供者)の関与についての証拠性を高めるために，証跡情報に対して当事者によるデジタル署名を生成する場合，証跡情報が生成されるタイミングにおいて，当事者が署名の意志を持って署名生成できることが求められることから，証跡情報の収集シーケンスやサービスのシーケンスに対する影響を極力抑制しながら証跡情報への署名生成を実行するための技術が求められる. また, 上記で生成された署名の検証においては, 一般に公開鍵証明書の信頼パスや各証明書の失効の有無を確認するための処理が必要となるなど，オーバーヘッドの大きい処理となることから，証跡情報の収集処理や，サービスに対する性能への影響を極力抑制した署名検証技術が求められる．またタイムスタンプについても，その取得タイミングや取得したタイムスタンプの検証において, 上記と同様の要件が求められる.

(2)署名データの長期有効性の維持

収集した証跡情報は，後日，その証跡情報をもとにサービス事実証明の必要性が発生するまで，その真正性が維持されている必要がある.

利用者やサービス提供者等の当事者のデジタル署名を付与した証跡情報を残す場合，一般にデジタル署名の有効性には期限が存在することから，デジタル署名の有効性を長期にわたり維持するための長期署名技術[4]-[6]を，署名が付与された証跡情報に対して確実に適用するための管理技術が求められる.

5 まとめ

サービス事実証明のための証跡管理の必要性を述べ, その実現に向けた検討の1つとして, 収集管理すべき証跡情報についての検討を行った. その結果, サービス事実の証明に求められる証跡情報に対する特有な要件として, (1)複数証跡情報によるサービス事実の証明, および(2)証跡情報に対する客観性の向上 の考慮が必要であることを述べた.

さらに上記要件を満たすために, 証跡管理基盤に求められる技術要件について述べた.

今後は, 事実証明対象のサービス形態の違いに応じた証跡情報に対する要件への影響や, 4.で挙げた技術要件を満たすための課題およびその解決等について検討を深めていく.

参考文献

[1] 福田, 溝渕ら, “ネットワークフォレンジックのためのホスト型のロギングについて”, 2009 年 電子情報通信学会総合大会, AS-1-3, 2009

[2] 芦野, 藤田, 入澤, 佐々木, “デジタルデータ証拠保全プラットフォーム『Dig-Force シリーズ』の開発と評価, DICOMO2008, 2008

[3] 間形, 高橋, 金井, ”デジタル証拠の法的証明力を高めるための要件に関する一考察”, 電子情報通信学会 SCIS2008, 4E1-6, 2008

[4] JIS X 5092:2008 CMS 利用電子署名(CAdES)の長期署名プロファイル, 2008

[5] JIS X 5093:2008 XML 署名利用電子署名(XAdES)の長期署名プロファイル, 2008

[6] ECOM, “電子文書長期保存ガイドブック”, http://www.ecom.jp/results/h18seika/h18results-17.pdf, 2007